MATH 370 Lecture 3

GROUPS

Recall from last time that we discussed binary operations.

Definition of a group:

A group is a set G together with a binary operation $*$ such that:

i) $*$ is associative, i.e $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for every $g_1, g_2, g_3 \in G$

ii) Existence of identity There exists a $e \in G$ such that $g * e = e * g = g \quad \forall g \in G$

iii) Existence of inverse For every $g \in G$, there exists $g^{-1} \in G$ such that

$$g * g^{-1} = g^{-1} * g = e$$

Examples: i) $(S_n, \circ)$ ii) $(A_n, \circ)$

iii) $(\mathbb{R}, +)$ iv) $(\mathbb{Q}, +)$ v) $(\mathbb{Z}, +)$

vi) Roots of unity

$$G_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$$

$$G_2 = \{ \pm 1 \}$$

$$G_3 = \{ 1, w, w^2 \} \qquad w = e^{2\pi i/3}$$

$$G_4 = \{ \pm 1, \pm i \}$$

$$\vdots$$

$$G_n = \{ e^{2\pi i k/n} \mid k \in \{0, 1, \ldots, n-1\} \}$$

Abelian Groups

Defn: A group $(G,*)$ is called abelian if

$$g_1 * g_2 = g_2 * g_1 \quad \forall \; g_1, g_2 \in G.$$

Exc: In previous examples, which groups were abelian?

Some useful properties of groups

Let $(G,*)$ be a group.

i) $e \in G$ is unique.

Suppose there are two identities say e_1 & e_2. Then

$$e_1 * e_2 = e_1$$
$$= e_2$$

So, $e_1 = e_2$.

ii) Given a $g \in G$, g^{-1} is unique.

Suppose there are two elements g_1 & g_2 such that

$$g_1 * g = g * g_1 = e \quad \text{—} \quad (1)$$

& $$g_2 * g = g * g_2 = e \quad \text{—} \quad (2)$$

Consider (1) & multiply the entire equation with g_2

$$(g_2 * g_1) * g = (g_2 * g) * g_1 = e * g_1 = g_1$$

Also $$(g_2 * g_1) * g = g_2 * (g_1 * g) = g_2 * e = g_2$$

So, $g_1 = g_2$.

iii) Cancellation property

If $gh = gf$, then $h = f$

$$gh = gf$$

Multiply with g^{-1}; $\Rightarrow g^{-1}(gh) = g^{-1}(gf)$

$$h = f.$$

Similarly one can show that if $hg = fg$ then $h = f$.

SUBGROUPS

Let $(G, *)$ be a group.

Defn: We say that a subset $H \subseteq G$ is a **Subgroup** of $(G, *)$ if:

i) $*$ restricted to H is a binary operation on H

ii) $e \in H$ iii) For every $h \in H$, $h^{-1} \in H$.

Example:

$$(\mathbb{R}, +) \supseteq (\mathbb{Q}, +) \supseteq (\mathbb{Z}, +)$$

$$\cap |$$

$$(\mathbb{C}, +)$$

What about $(\mathbb{R} - \{0\}, +) \subseteq (\mathbb{R}, +)$?

$(A_n, \cdot) \subseteq (S_n, \cdot)$

$(SL_n(\mathbb{R}), \cdot) \subseteq (GL_n(\mathbb{R}), \cdot)$

Order of an element in group

Let $g \in G$.

Defn: We say that n is order of g, denoted by $\text{ord}(g)$ if n is the smallest number such that $\underbrace{g * g * g \cdots * g}_{n \text{ times}} = e$

(can also write as g^n)

Example: $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$\text{ord}(e) = 1$

$\text{ord}((12)) = 2 \qquad (12)(12) = e$

$= \text{ord}((13))$

$= \text{ord}((23))$

$\text{Ord}((123)) = 3 = \text{Ord}((132))$

$(123)(123) = (132)$

$(132)(123) = e$

$\rightarrow$ Ord (cycle of length n) $= n$

Lemma: Suppose G is a finite group. Then every $g \in G$ has finite order.

Pf: Suppose not, i.e. there exists a $g \in G$ that has infinite order.

$\Rightarrow g^i \neq g^j$ where $i, j \in \mathbb{N}$, $i \neq j$

because if $g^i = g^j$ then either

$g^{i-j} = e$ or $g^{j-i} = e$

which is a contradiction.

So, $\{g, g^2, g^3, g^4, \ldots\} \subseteq G$

which is a contradiction.

CYCLIC GROUPS

Defn: We say that a group G is **cyclic** if $\exists\ g \in G$ s.t

$$G = \{g^i \mid i \in \mathbb{Z}\}$$

Can also denote G as $\langle g \rangle$.

$i = 0 \quad g^i = e$

$i > 0 \quad g^i = \underbrace{g * g * \cdots * g}_{i \text{ times}}$

$i < 0 \quad g^i = (g^{-i})^{-1}$

$|G| < \infty \iff \text{ord}(g) \in \mathbb{N}$

$|G| = \infty \iff g$ has infinite order.

Example: $(\mathbb{Z}, +) = \langle 1 \rangle$

$$A_3 = \langle (123) \rangle$$

n-th roots of unity $= \langle e^{2\pi i/n} \rangle$

GROUP HOMOMORPHISMS

Defn: A group homomorphism $\varphi: G_1 \to G_2$ is a map satisfying

$$\varphi(gh) = \varphi(g)\,\varphi(h)$$

Lemma: $\varphi(e_{G_1}) = e_{G_2}$

Pf: $\varphi(e_{G_1}) = \varphi(e_{G_1} e_{G_1}) = \varphi(e_{G_1})\,\varphi(e_{G_1})$

Multiply with $\varphi(e_{G_1})^{-1}$ to get

$$e_{G_2} = \varphi(e_{G_1})$$

Examples: 1) $G_1 = (GL_n(\mathbb{R}), \cdot)$

$$G_2 = (\mathbb{R} - \{0\}, \cdot)$$

$$\det : G_1 \to G_2$$

b/c $\det(AB) = \det(A)\det(B)$

2) Recall that in lecture 2, we defined Signature of a permutation,

$$\varepsilon: S_n \longrightarrow \{\pm 1\}$$

It is also a group homomorphism b/c

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$$

3) $$\exp: (\mathbb{R}, +) \longrightarrow (\mathbb{R} - \{0\}, \cdot)$$

$$r \longmapsto e^r$$

$$\exp(r_1 + r_2) = e^{r_1 + r_2} = e^{r_1} e^{r_2} = \exp(r_1)\exp(r_2)$$

Lemma: Let G be a group. There is atleast one homomorphism from $(\mathbb{Z}, +)$ to G.

Pf: Choose $g \in G$ and fix this choice.

Define $\varphi_g : (\mathbb{Z}, +) \longrightarrow G$ as follows

$$\varphi_g(0) = e$$

$$\varphi_g(1) = g$$

$m > 0 \qquad \varphi_g(m) = g^m$

$m < 0 \qquad \varphi_g(m) = (\varphi_g(-m))^{-1} = (g^{-m})^{-1}$

For $m, n \in \mathbb{Z}$

$$\varphi_g(m+n) = g^{m+n} = g^m g^n$$

$$= \varphi_g(m)\ \varphi_g(n)$$

Lemma: A group homomorphism maps inverses to inverses.

Pf: Let $\varphi: G_1 \longrightarrow G_2$ be group hom.

We want to show that

$$\varphi(g_1^{-1}) = (\varphi(g_1))^{-1}$$

$$\varphi(g_1)\ \varphi(g_1^{-1}) = \varphi(g_1 g_1^{-1}) = \varphi(e)$$

$$= e$$

Hence, done.

Group homomorphisms give rise to two important subgroups image & kernel.

Defn: (1) kernel

$\varphi: G_1 \to G_2$ group hom

$$\ker \varphi = \{ g \in G_1 \mid \varphi(g) = e \}$$

(2) image

$$\text{im}\varphi = \{ \varphi(g) \mid g \in G_1 \}$$

By definition $\ker \varphi \subseteq G_1$

$\text{im}\varphi \subseteq G_2$.

Lemma: $\text{im}\varphi$ & $\ker \varphi$ are subgroups.

Pf: Let us show that $\ker \varphi \subseteq G_1$ is a subgroup.

i) Suppose $g, h \in \ker \varphi$, want to show that $gh \in \ker \varphi$.

$$\varphi(gh) = \varphi(g)\,\varphi(h) = e^2 = e$$

ii) $e \in \ker\varphi$ because $\varphi(e) = e$.

iii) If $g \in \ker\varphi$, then $\varphi(g^{-1}) = \varphi(g)^{-1}$
$= e^{-1}$
$= e$

So, $g^{-1} \in \ker\varphi$.

Hence, $\ker\varphi$ is a subgroup.

Let us now show that $\operatorname{im}\varphi$ is a subgroup of G_2.

i) Suppose $g_1, g_2 \in \operatorname{im}\varphi$

i.e. $g_1 = \varphi(h_1)$

$g_2 = \varphi(h_2)$

$g_1 g_2 = \varphi(h_1)\,\varphi(h_2) = \varphi(h_1 h_2)$

So $g_1 g_2 \in \operatorname{im}\varphi$.

ii) $e = \varphi(e)$, so $e \in \operatorname{im}\varphi$

iii) If $g \in \operatorname{im}\varphi$, say $g = \varphi(h)$ then

$$g^{-1} = \varphi(h)^{-1} = \varphi(h^{-1})$$

So, $g^{-1} \in \operatorname{im}\varphi$.

Examples:

1) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R} - \{0\}$

$\text{Kernel} = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$

$= SL_n(\mathbb{R})$

$\text{image} = \mathbb{R} - \{0\}$

b/c Say $a \in \mathbb{R} - \{0\}$ $\quad a = \det \begin{pmatrix} a & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$

2) $\varepsilon : S_n \longrightarrow \{\pm 1\}$

$\operatorname{im}\varepsilon = \{\pm 1\}$

$\ker \varepsilon = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} = A_n$

3) $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}-\{0\}, \cdot)$

$$r \longmapsto e^r$$

$$\operatorname{im} \exp = \{ r \in \mathbb{R}-\{0\} \mid r > 0 \}$$

$$\ker \exp = \{ r \in \mathbb{R} \mid e^r = 1 \}$$

$$= \{0\}$$